

(12) **United States Patent**
Ketari

(10) **Patent No.:** **US 9,313,313 B2**
(45) **Date of Patent:** **Apr. 12, 2016**

(54) **PROXIMITY ACCESS AND/OR ALARM APPARATUS**

(76) Inventor: **Nissaf Ketari**, Tunis (TN)
(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1156 days.

(21) Appl. No.: **12/198,218**

(22) Filed: **Aug. 26, 2008**

(65) **Prior Publication Data**
US 2010/0022217 A1 Jan. 28, 2010

Related U.S. Application Data

(63) Continuation-in-part of application No. 12/177,495, filed on Jul. 22, 2008.

(51) **Int. Cl.**
H04B 7/00 (2006.01)
H04M 1/66 (2006.01)
H04M 1/60 (2006.01)
H04W 88/06 (2009.01)

(52) **U.S. Cl.**
CPC **H04M 1/66** (2013.01); **H04M 1/6066** (2013.01); **H04M 2250/02** (2013.01); **H04W 88/06** (2013.01)

(58) **Field of Classification Search**
CPC H04W 12/08; H04W 48/08; H04W 84/18; H04W 84/20; H04W 92/00
USPC 455/411, 41.2, 41.3, 410; 340/686.6
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,449,651 B1 *	9/2002	Dorfman et al.	709/229
6,885,848 B2 *	4/2005	Lee	455/41.2
7,259,671 B2 *	8/2007	Ganley et al.	340/539.23
7,526,293 B2 *	4/2009	Kim et al.	455/456.2
2004/0153659 A1 *	8/2004	Naccache et al.	713/193
2004/0203590 A1 *	10/2004	Shteyn	455/410
2007/0061893 A1 *	3/2007	Black et al.	726/27
2007/0254588 A1 *	11/2007	Lafuente	455/41.2
2007/0256126 A1 *	11/2007	Erickson et al.	726/20
2007/0273643 A1 *	11/2007	Erez et al.	345/156
2008/0081667 A1 *	4/2008	Parikh et al.	455/558
2008/0301466 A1 *	12/2008	Hsu et al.	713/189
2008/0318561 A1 *	12/2008	Olshansky et al.	455/417
2009/0207014 A1 *	8/2009	Ayed	340/539.13
2009/0249478 A1 *	10/2009	Rosener et al.	726/19

* cited by examiner

Primary Examiner — Christopher M Brandt

(74) *Attorney, Agent, or Firm* — Daniel Schein, Esq.

(57) **ABSTRACT**

A method and system for securing portable electronic devices as well as access to data on the portable electronic device is described.

The method consists of a proximity alarm that alarms if the physical device is carried away from the user mobile phone, or from some fixed stations.

The method consists of separating the keys from the storage device where the data is stored by storing them on a FOB.

When access to data is requested, the key is reconstituted in real-time by wirelessly obtaining data from the FOB and from the user, and the data is decrypted.

The system provides for secure transmission of keys in real-time, and provides safeguards in case of breach of security.

19 Claims, 11 Drawing Sheets

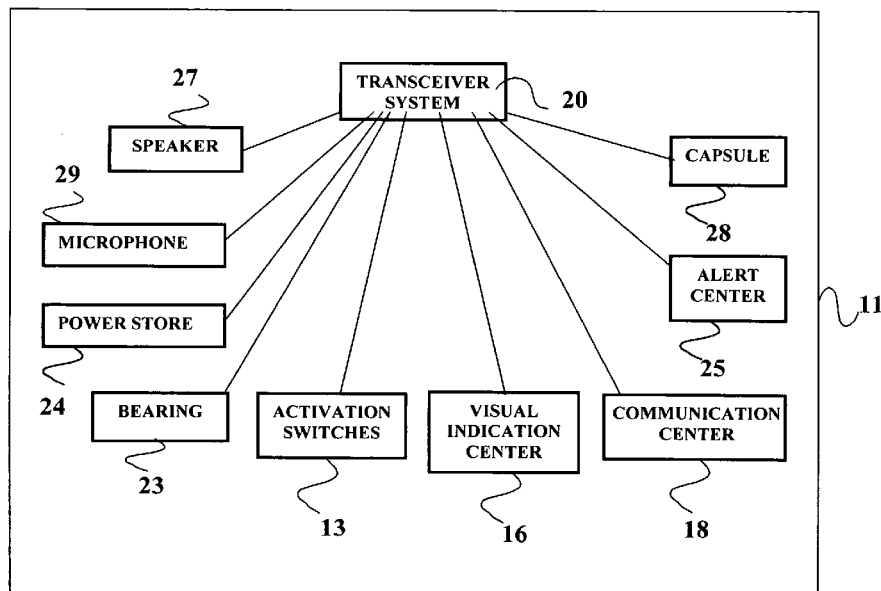


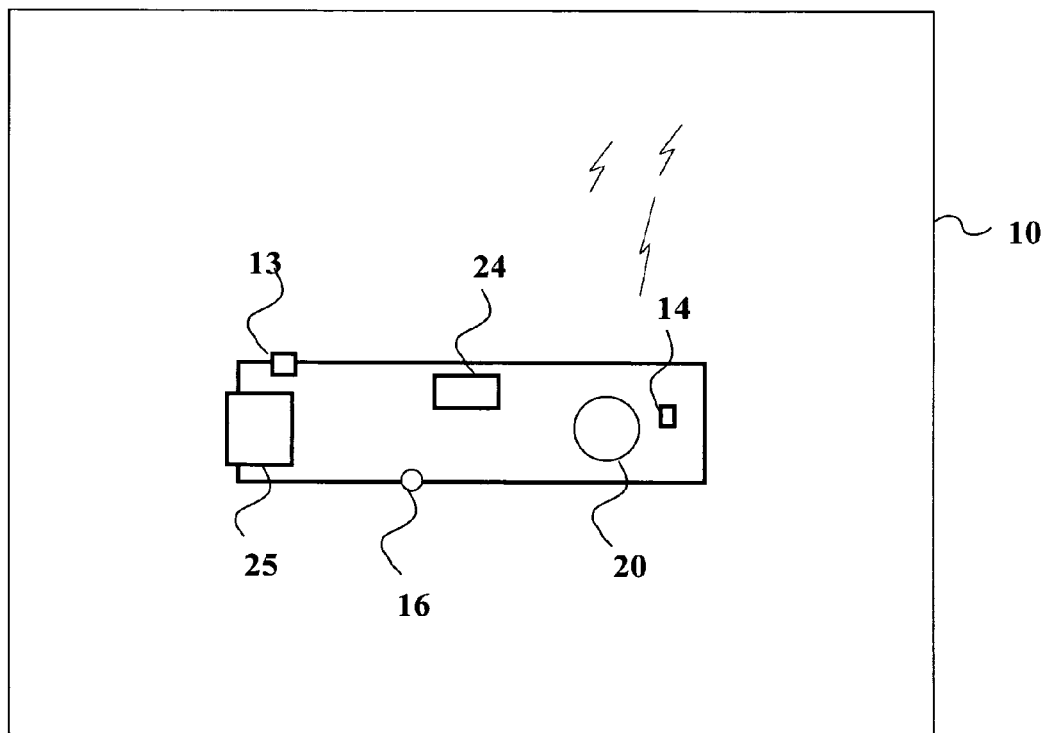
Fig. 1A

Fig. 1B

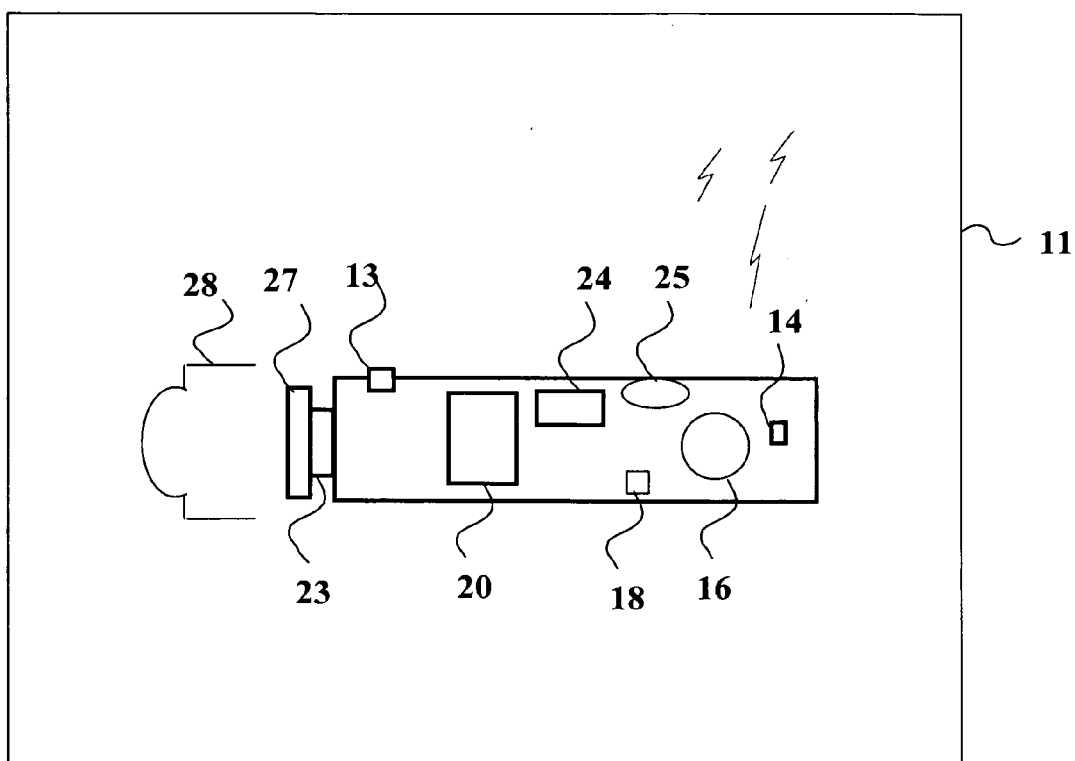


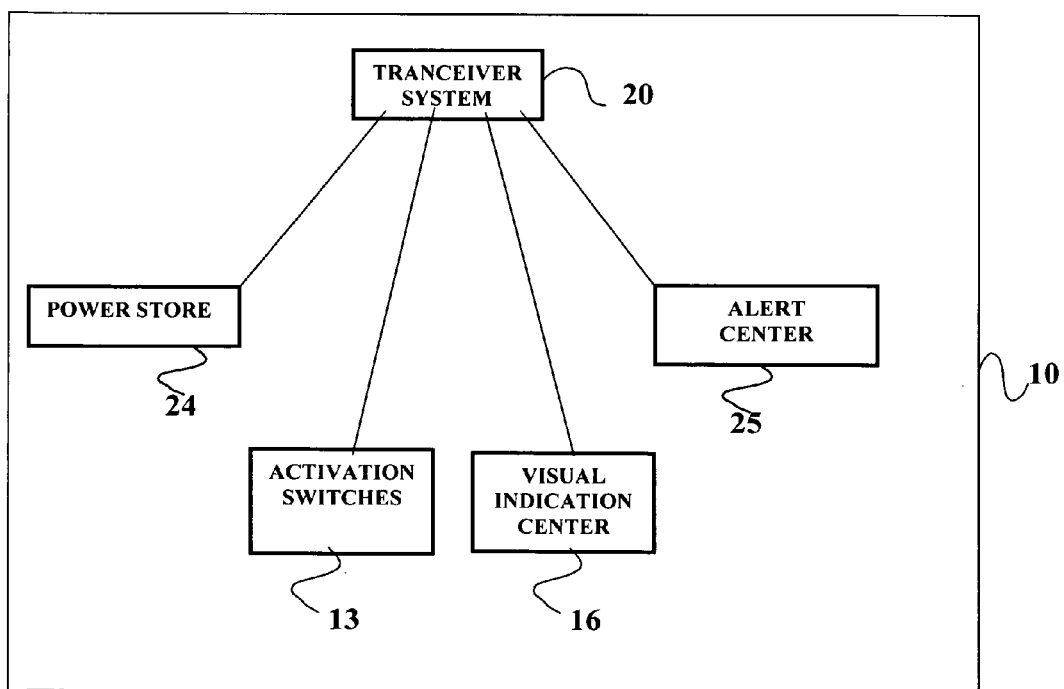
Fig. 2A

Fig. 2B

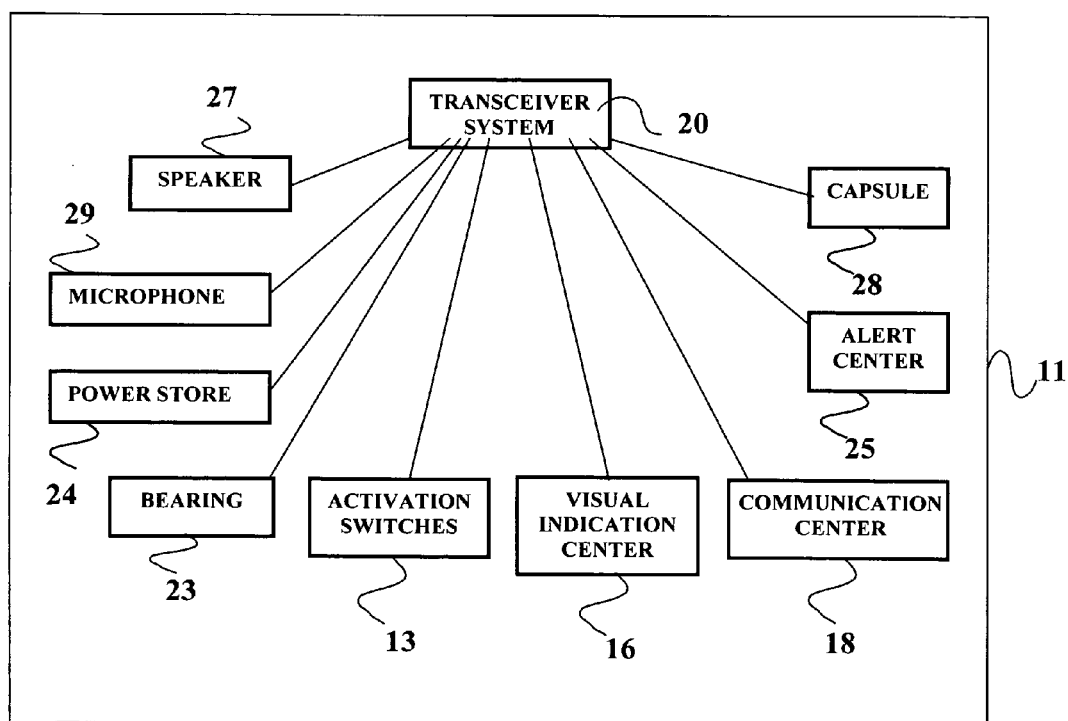


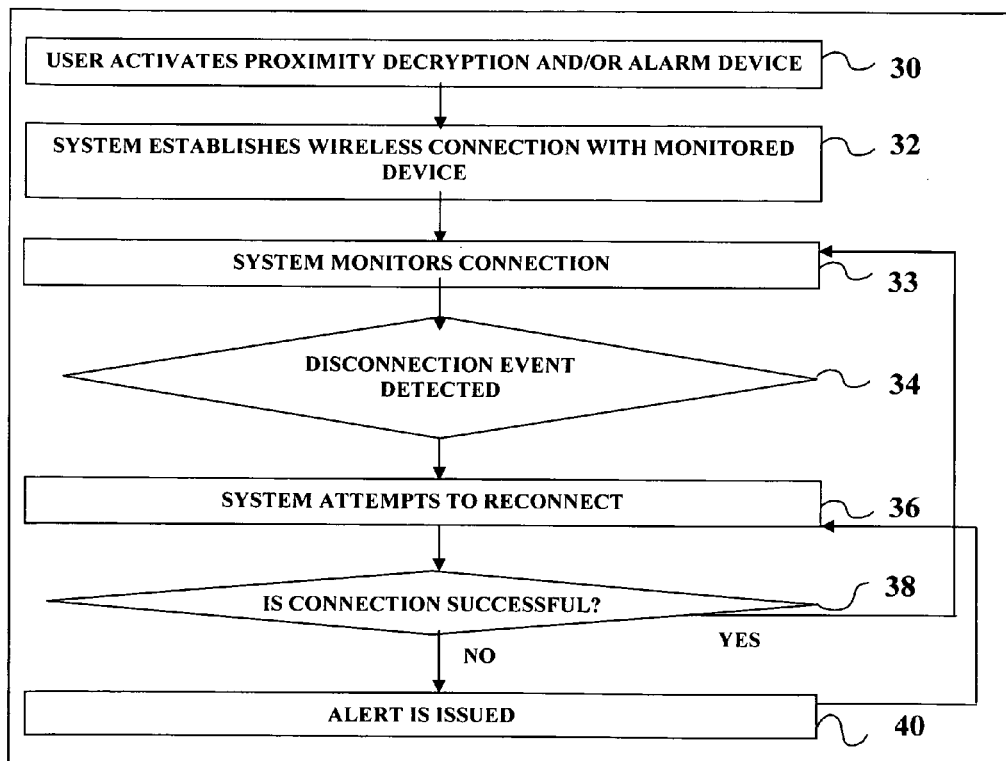
Fig. 3A

Fig. 3B

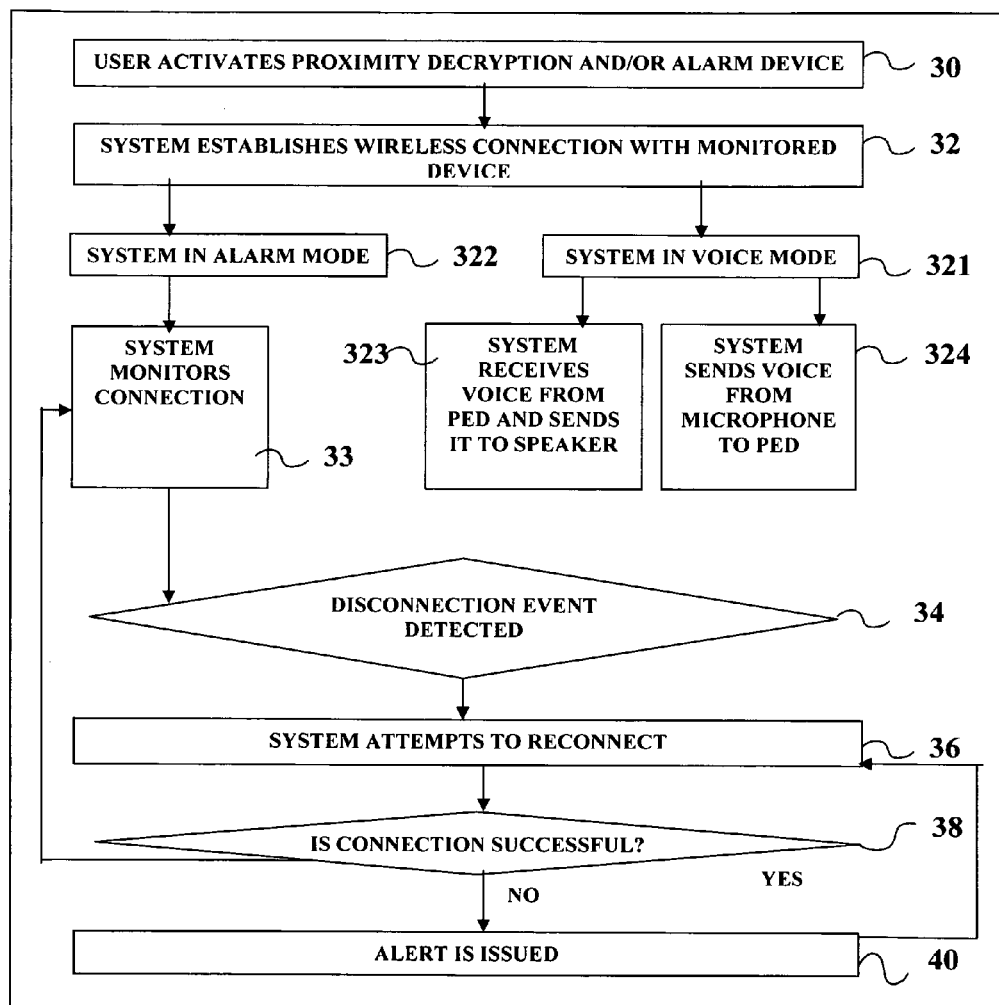


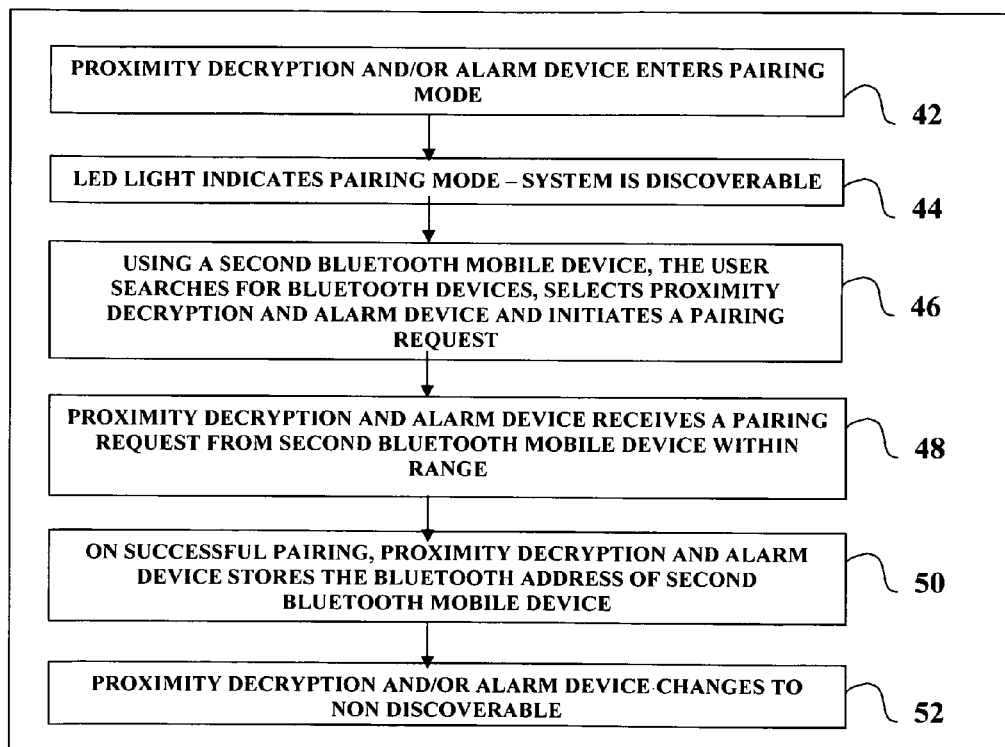
Fig. 4

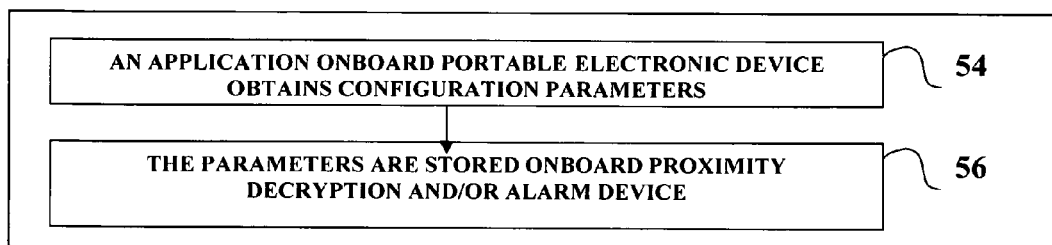
Fig. 5

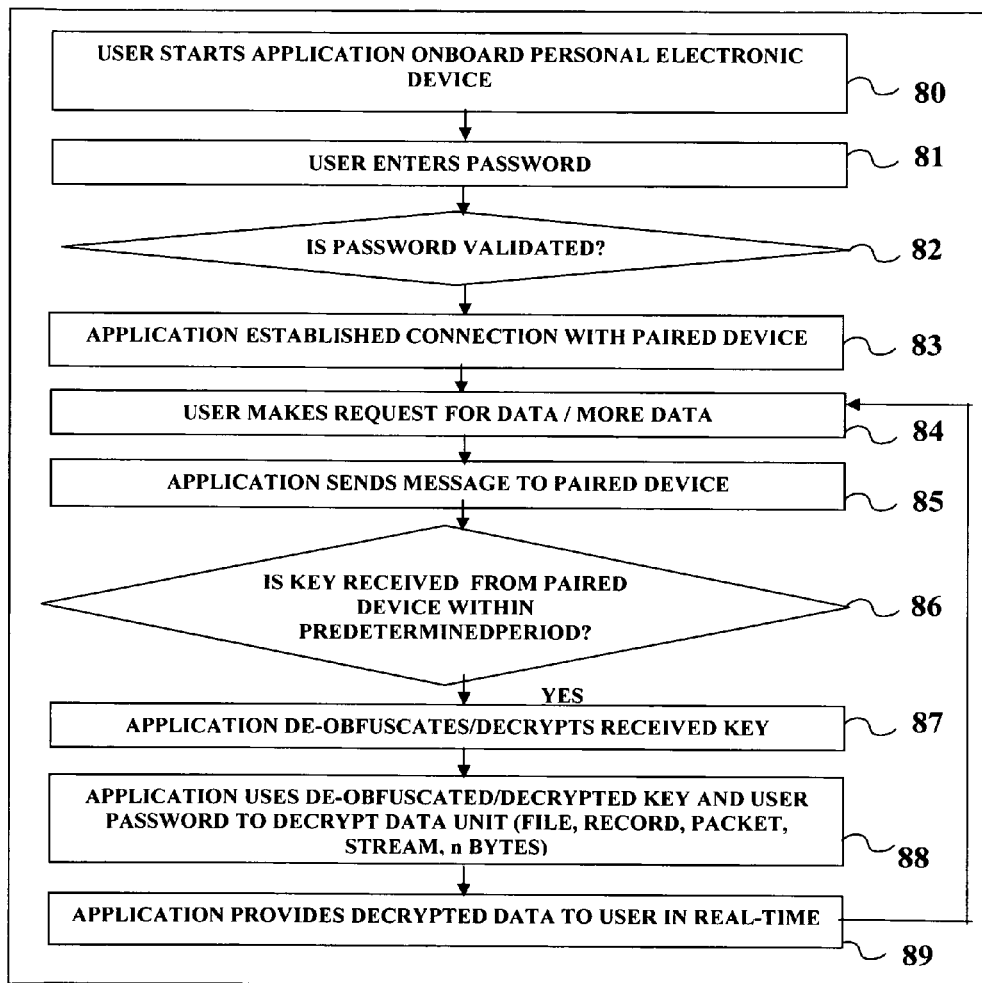
Fig. 6

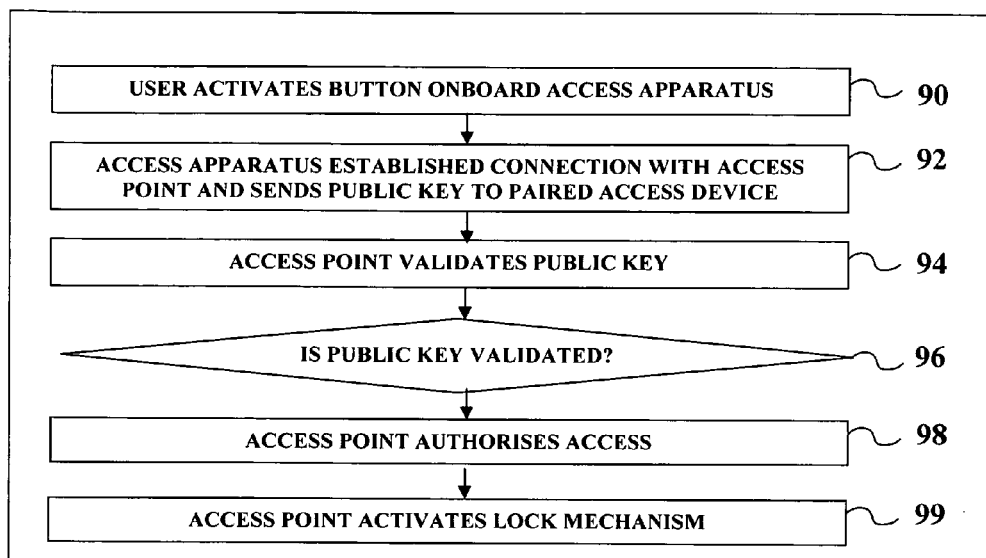
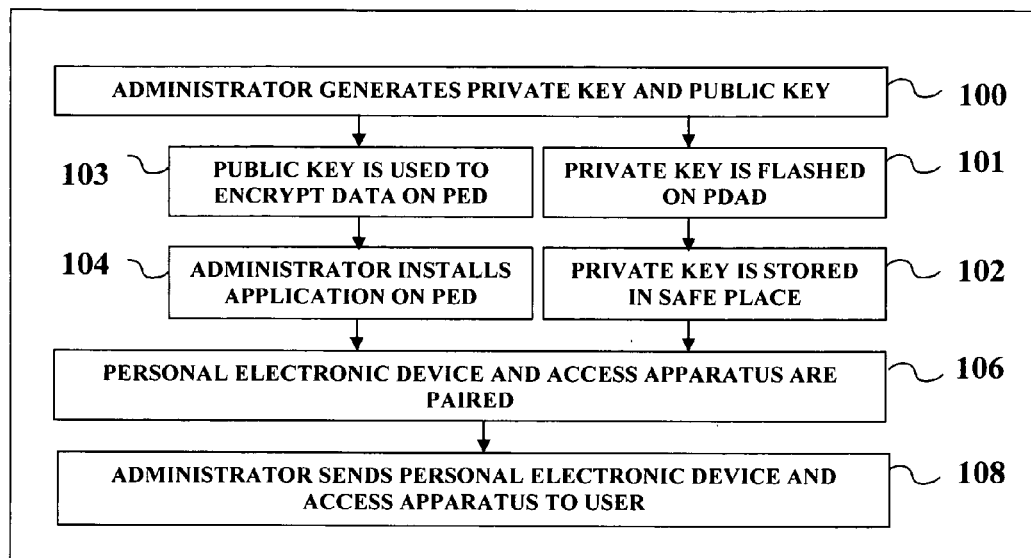
Fig. 7

Fig. 8

**PROXIMITY ACCESS AND/OR ALARM
APPARATUS****PRIORITY**

The present application is a Continuation-In-Part ("CIP") of pending U.S. patent application Ser. No. 12/177,495, filed Jul. 22, 2008.

FIELD OF THE INVENTION

The present inventions relate to wireless security and more specifically relates to a proximity access device.

BACKGROUND

More and more personal data is being stored on ever smaller and more mobile devices. The risk that sensitive data regarding identity, access codes, or business information could be compromised if one of these devices is misplaced increases with the amount of information that can be stored on them and their increasingly pervasive use. Requiring the entry of security codes or keys is a partial solution, but the efficacy of this solution decreases to the extent that the data onboard the device can be used if the mobile device lands in the wrong hands.

Portable electronic devices such as cellular telephones, personal digital assistants (PDAs), wireless email devices, instant messaging devices, pagers, portable compact disk (CD) players, portable MP3 players, and others are often forgotten, lost, or stolen (a "PED" includes any portable device that can be used for communication, performing intellectual and/or physical work, and/or entertainment).

Current data protection solutions consist of:

Password authentication,

User passwords are generally short and can be bypassed by reinstalling the operating system or the application. Passwords can be hacked through several methods including guessing, observation, and installing Trojan Horses (A virus in which malicious or harmful code is contained inside apparently harmless programming or data).

File encryption and decryption on entry of a password,

Some market available applications allow the user to define a password and to select an encryption method and an encryption key length. This application generally does either a bulk encryption or a file encryption on saving and a decryption on user opening a file.

In this method, the decryption key is generally encrypted and stored on the same computer as the encrypted data; this is analogous to locking a safe, and hiding the safe key under the door of the safe. Not only that, the decryption key is generally decrypted when the user enters a short password (generally less than 10 digits) and stored in a fixed location in memory during the whole duration of the user session and is used every time a file requires decryption.

A malicious program can find the decryption key and make it available to a hacker. Furthermore, recent techniques of cooling memory can make the decryption key available to a hacker for a period following system shut down.

SECUREID code for access to network,

SECUREID is cumbersome and inconvenient for the user. SECUREID is good at protecting a server from unauthorized access, and at validating users over a network. However, it fails to work in un-networked environment, and can have response latency.

USB dongle,
USB dongle is used to authenticate a user through the presence of a hardware device with a specific ID. USB dongles can be duplicated by experts.

5 PCs software like LOCKITNOW™ provides the ability to pair a computer with a mobile phone, and have the Windows login unlock when the user is in proximity and lock when the user is out of proximity.

RFID Key

10 Some high end cars provide RFID keys for contactless door access and engine start.

Another method for protecting data onboard a personal electronic device (PED) is disclosed in U.S. patent application 60/199,538, titled: Automatic data encryption and access control based on BLUETOOTH device proximity which decrypts data on contact with a paired BLUETOOTH device, and encrypts the data on loss of contact. This method is inefficient, can cause data corruption, and more importantly, it does not provide high level security. The Bluetooth ID of paired Bluetooth device can be obtained from the operating system, and can be used to fake the BLUETOOTH device.

20 It is noted that PED can refer to a computer, a mobile phone, a handheld device, an information system, a vehicle electronic computer, or any electronic system.

US Patent application publication 20050280546 discloses two mobile transceivers that are linked through a BLUETOOTH link. The BLUETOOTH enabled RF link between the first and second mobile transceiver units forms a monitoring piconet. The second mobile transceiver unit provides an alarm indication when the first mobile transceiver unit moves beyond a distance of approximately ten meters from the second mobile transceiver unit. The second device repeatedly pages the first device, and waits for a response. If a response is not received, an alarm is issued. This method has been tested and found to be unreliable due to high energy consumption and due to the human body blocking Bluetooth signals.

35 U.S. Pat. No. 6,885,848 is directed to an apparatus for preventing the loss of a portable telephone that uses BLUETOOTH communication protocol. The signal strength is periodically monitored and an alarm issued to the headphone when the signal is below a threshold. BLUETOOTH protocol provides for a received signal strength indicator (RSSI) value or the Link Quality value to be determined at any time. If the value received is below a threshold, an alarm is issued to the headphone. This system may reduce the chance that a portable telephone is lost or stolen, but if the mobile phone falls in the wrong hands, this system does not prevent the data from being accessed.

Thus, a need exists for a method and apparatus for securing assets and sensitive data on them that are reliable, simple to use, cost effective, mobile, adaptable and secure that consists of: Separating the location of encrypted data and encryption key. Data should be encrypted at all times, and should be decrypted in memory only when it is requested by the user and after wirelessly validating security credentials. The key should be personalized, non-sharable. An administrator should be able to initialize, distribute and manage the keys remotely. An administrator should be able block and to replace keys in case of loss or theft without compromising the security of a number of devices and without compromising access to existing data.

SUMMARY OF THE INVENTION

Event-based Real-time decryption on the fly, of a fixed-size set of data, with no storing of decrypted data on disk, using a FOB that comprises only a single Bluetooth transceiver IC.

3

A unitary apparatus, comprising: a power input; a single transceiver selected from the set comprising a BLUETOOTH or Wibree transceiver, wherein said single transceiver can pair with a second apparatus in a first range, wherein on receipt of a connection request from said paired second apparatus, said single transceiver establishes a secure two-way wireless connection with said paired second apparatus, wherein on receipt of a first digital message from said paired second apparatus, said single transceiver automatically transmits a second digital message.

A method for real-time decryption of sensitive data onboard a personal electronic device comprising: pairing said personal electronic device with a unitary apparatus comprising a single transceiver in a first range, said single transceiver is selected from the set comprising a BLUETOOTH and a Wibree transceiver, upon user requesting sensitive data from storage device, said storage device is selected from the set comprising: solid state memory, USB flash, disk drive, network drive, external drive, CD ROM, ZIP drive, Flash drive, Bluetooth drive, a request for a digital code is transmitted wirelessly to said unitary apparatus comprising a single transceiver, on receipt of said digital code from said unitary apparatus, said digital code is authenticated, on successful authentication, said sensitive data is decrypted, said decrypted sensitive data is presented to said user.

A method for managing sensitive data comprising: generating private key and associated public key for a user, storing said private key and said public key in a database, flashing said public key to a second apparatus with a single transceiver selected from the set comprises of Bluetooth and Wibree transceivers, encrypting sensitive data using said private key for said user, transferring said encrypted sensitive data to said user storage device.

BRIEF DESCRIPTION OF THE FIGURES

The present inventions may be more clearly understood by referring to the following figures and further details of the inventions that follow.

FIG. 1A is a schematic of a proximity access and/or alarm device.

FIG. 1B is a schematic of an alternative proximity access and/or alarm device.

FIG. 2A is a block diagram of proximity access and/or alarm device.

FIG. 2B is a block diagram of an alternative proximity access and/or alarm device.

FIG. 3A is a flowchart illustrating the operation of a proximity access and/or alarm device.

FIG. 3B is a flowchart illustrating an alternative operation of a proximity access and/or alarm device.

FIG. 4 is a flowchart illustrating initiating the proximity access and/or alarm device.

FIG. 5 is a flowchart illustrating configuring the proximity access and/or alarm device.

FIG. 6 is a flowchart illustrating an alternative embodiment for providing secure access to sensitive data.

FIG. 7 is a flowchart illustrating the operation of a Bluetooth key.

FIG. 8 is a flowchart illustrating an embodiment for setting up the system.

4

Similar reference numerals are used in different figures to denote similar components.

FURTHER DETAILS OF THE INVENTIONS

The following provides further details of the present inventions summarized above and illustrated in a schematic fashion in the Figures. In accordance with a first aspect of the present inventions, FIG. 1A is a schematic illustration of a proximity access and/or alarm device (PAAD) 10 comprising a transceiver system 20 operatively connected with at least one activation switch 13, a visual indication center (or display) 16, a power store 24, a communication center 25 and an antenna 14. Display 16 can be used to indicate the status of the device, such as whether it is powered, if the BLUETOOTH transceiver system (BT) is discoverable or non-discoverable, if the BT is pairing or paired with another BT, the BT mode, inter alia.

In a preferred embodiment, the components of the PAAD 10 can fit in a volume less about 60×30×10 mm or 18 cc, so that PAAD 10 can fit into a housing having an interior with dimensions of 60×30×10 mm or no more than 18 cc. In another embodiment, PAAD 10 can fit into a volume 10 cc, and weigh about 50 grams or less, and preferably less than about 10 g. Devices of the present invention should take up minimal volume and be light weight. For example, each device of the present inventions will preferably fit into a space having a volume of 56 cubic centimeters, 25 cubic centimeters, 22.5 cubic centimeters, 18 cubic centimeters, 10 cubic centimeters, or 1 cubic centimeters, and each device of the present inventions preferably has a weight less than about 200 grams, less than about 50 grams, or less than about 10 grams.

An attachment mechanism or system, including but not limited to a hook, harness, notebook security lock, insert, pin, clip, badge, clip, key chain, car key, firearm activation key, ring, tee, dog collar, Velcro, ring, fastening mechanism, sticky surface are optionally attached to PAAD 10.

Control or activation switches 13 can be any type of button, switch, remote sensor, touch sensor, contact sensor, bio sensor, key pad to enter password or activation system. Activation switches 13 are used to turn the PAAD 10 ON/OFF, to shut off the alarm of communication center 25. For example, a single control button can cycle through a menu of functions by changing the length of time that the button is held and/or the speed with which a first press is followed by a second press (analogous to the single and double click on a computer mouse). One or two control buttons coupled with a simple display screen can adjust a variety of operational parameters.

Transceiver system 20 is preferably a Bluetooth transceiver. In an alternative embodiment, transceiver 20 can be Wibree or Wifi. Transceiver 20 enables connectivity over the 2.4 GHz radio frequency (RF) band. Transceiver system 20 includes a radio and base band IC/integrated circuit for BLUETOOTH 2.4 GHz systems. BLUETOOTH ICs are generally available from manufacturers such as CSR or Broadcom, and comprises a full system including baseband, processor, RF front end, RAM/Flash/ROM.

In a preferred embodiment, transceiver system 20 includes ROM, Flash memory or external memory or any other type of memory. In an alternative embodiment, transceiver system 20 includes a power amplifier (PA) and/or low noise amplifier (LNA) for increasing the BLUETOOTH transmission range. In a preferred embodiment, transceiver system 20 includes a processor, RAM and Flash. Software/firmware can be loaded on Flash using SPI flashing. The processor executes the BLUETOOTH protocol, as well as the firmware that provides custom functionality (example: proximity detection, alarm-

5

ing functionality, applying transformations, transferring keys . . .). The processor can also execute other functionality such as sending files on pairing, flashing lights, providing voice functionality, relaying voice to a remote BLUETOOTH device, detecting connection from a remote BLUETOOTH device, etc.

The BLUETOOTH specification (a de facto standard containing information required to ensure that devices supporting BLUETOOTH can communicate with each other worldwide) defines two transmission ranges for personal area networking. The range is between 10 m and 100 m without a line of sight requirement. The radio link is capable of voice and data transmission up to a maximum capacity of 720 kbps per channel. Any other range can be designed.

A BLUETOOTH network is completely self organising, and ad hoc personal area networks (PANs) can be established wherever two or more BLUETOOTH/Wibree/Wifi devices are sufficiently close to establish radio contact. Equipment capable of BLUETOOTH connectivity is able to self-organise by automatically searching within range for other BLUETOOTH-enabled devices. Upon establishing a contact, information is exchanged which determines if the connection should be completed or not. During this first encounter, the BLUETOOTH devices connect via a process of authorisation and authentication.

BLUETOOTH Pairing happens when two BLUETOOTH enabled devices authenticate each other and agree to communicate with one another. When this happens, the two devices join what is can be referred to as a trusted pair. When one device recognizes another device in an established trusted pair, each device automatically accepts communication, bypassing the discovery and authentication process that normally happen during BLUETOOTH interactions. After pairing, each device may store the Bluetooth ID of the second device for future use.

When BLUETOOTH pairing is being set up, the following usually happens:

1. Device A (such as a handheld) searches for other BLUETOOTH enabled devices in the area.

How does A find these devices? The devices that are found all have a setting that makes them discoverable when other BLUETOOTH devices search. It's like raising your hand in a classroom: the discoverable devices are announcing their willingness to communicate with other BLUETOOTH devices. By contrast, many BLUETOOTH devices can toggle their discoverability settings off. When discoverability is off, the device will not appear when other devices search for it. Undiscoverable devices can still communicate with other BLUETOOTH devices, but they must initiate all the communications themselves.

2. A detects Device B (such as a second handheld that's discoverable).

During the discovery process, the discoverable devices usually broadcast what they are (such as a printer, a PC, a mobile phone, a handheld, etc.), and their BLUETOOTH Device Name (such as "Bob's Laptop" or "deskjet995c"). Depending on the device, you may be able to change the Device Name to something more specific. If there are 10 BLUETOOTH laptops and 5 BLUETOOTH mobile phones in range, and they are all discoverable, this can come in handy when selecting a specific device.

3. A asks B to send a Passkey or PIN

A passkey (or PIN) is a simple code shared by both devices to prove that both users agree to be part of the trusted pair. With devices that have a user interface, such as

6

handhelds, mobile phones, and PCs, a participant must enter the passkey on the device. With other types of devices, such as printers and hands-free headsets, there is no interface for changing the passkey on the device, so the passkey is always the same (hard coded). A passkey used on most BLUETOOTH headsets is "0000". The passkeys from both parties must match.

4. A sends the passkey to B

Once you've entered the passkey on A, it sends that passkey to B for comparison. If B is an advanced device that needs the user to enter the same passkey, it will ask for the passkey. If not, it will simply use its standard, unchanging passkey.

5. B sends passkey back to A

If all goes well, and B's passkey is the same entered by A, a trusted pair is formed. This happens automatically when the passkeys agree. Once a trusted pair is developed, communication between the two devices should be relatively seamless, and shouldn't require the standard authentication process that occurs between two devices who are strangers. Embodiments of the present inventions take advantage of the reduced power requirements of certain BLUETOOTH modes following pairing of two BLUETOOTH enabled devices.

BLUETOOTH has several types:

- i) Class 2: a class 2 BLUETOOTH transceiver can discover pair and communicate with any BLUETOOTH transceiver within a radius of 10 meters seamlessly.
- ii) Class 1: A class 1 BLUETOOTH transceiver can discover pair and communicate with any BLUETOOTH transceiver within a radius of 100 meters.
- iii) Class 3: A class 3 BLUETOOTH transceiver can discover pair and communicate with any BLUETOOTH transceiver within a radius of 2 meters.
- iv) Non standard devices: can be designed to discover pair and communicate with any BLUETOOTH transceiver within any distance less than 300 meters.

Bluetooth inquiry procedure enables a device to discover which devices are in range, and determine the addresses and clocks for the devices. The inquiry procedure involves a unit sending out inquiry packets (inquiry state) and then receiving the inquiry reply. The unit that receives the inquiry packets (the destination), will hopefully be in the inquiry scan state to receive the inquiry packets. The destination will then enter the inquiry response state and send an inquiry reply to the source. After the inquiry procedure has completed, a connection can be established using the paging procedure.

Paging Procedure is used to communication with another device directly using a device Bluetooth address. Paging allows sending packets to a specific Bluetooth device.

Power store 24 provides power to some of the components of PAAD 10. Power store 24 can be a capacitor, a battery (fuel cell, nickel-cadmium, lithium, lithium polymer, lithium ion, alkaline or nickel-hydride battery or any other portable source of electric power) or a combination of a capacitor and a battery, whereby the capacitor onboard a main unit is used to power transceiver system 20 for a number of utilizations and it can be charged from time to time by attaching the main unit to a detachable battery unit. Power store 24 can also be replaced with photovoltaic cells, a rechargeable battery, or a battery rechargeable from a distance (such as by induction). When PAAD 10 is not in operation it remains in a dormant state ("sleep-mode") to conserve the energy of power store 24. For example, small 1.5 volt batteries, and the like, such as those used in small devices like hearing aids, calculators and watches are widely available and can be used as for a power source. One of ordinary skill in the art can readily determine

the battery size and power requirements for different embodiments of the present inventions. It is envisioned that other low power specifications can be used in connection with the present inventions. For example, an ultra-low-power wireless technology called Wibree has been developed. Wibree addresses devices with very low battery capacity and can be easily integrated with BLUETOOTH technology.

Visual indication center **16** comprises one or more LED. The LED can turn on and off periodically to indicate the system is on. The color and frequency of the LEDs can indicate different events such as normal mode, pairing mode, alarm mode, low battery mode, voice mode, etc. In a preferred embodiment, visual indication center **16** while indicating the status of the system also illuminates a customizable face plate, made out of clear material such as acrylic. A logo or graphic can be printed on the face plate thus allowing to easily and economically change the look and branding of the device. This automatically leverages the visual indication center, and adds a promotional value and function to the device, above and beyond the main functions.

In another embodiment, visual indication center **16** can be an LCD or any other indication means, and communication center **25** includes an alarm audible from a distance greater than 3 feet. A regular alarm is between 65 and 120 decibels at 10 feet. Noise levels above 85 decibels can harm hearing over time. Noise levels above 140 decibels can cause damage to hearing after just one exposure. In a preferred embodiment, communication center **25** has more than 50 decibels or 50 dBA at 10 feet or exceeds ambient sound level by 5 decibels minimum. In a preferred embodiment, the alarm provides an audible signal of at least 60 decibels at 10 cm, or an audible alarm at 0.5 meter to notify the user of a designated event, such as a laptop or phone left behind. The human ear does not respond equally to all frequencies: humans are much more sensitive to sounds in the frequency range about 1 kHz to 4 kHz (1000 to 4000 vibrations per second) than to very low or high frequency sounds. Sound meters are usually fitted with a filter that has a frequency response similar to the human ear. If the "A weighting filter" is used, the sound pressure level is given in units of dB(A) or dBA. In residential areas, most noise comes from transportation, construction, industrial, and human and animal sources. Road traffic noise is the leading source of community noise. The noise can be highly variable. It is common that Day-Night sound levels in different areas vary over a range of 50 dB. The outdoor level in a wilderness area may occur as low as 30 to 40 dBA, and as high as 85-90 dBA in an urban area. Most urban dwellers live in areas of noise level more than 48 dBA.

Communication center **25** can be any type of audio, video, tactile or mechanical interface means capable of conveying information to the user. Communication center **25** can also be any type of data port, connector, USB connector, mini USB connector for exchanging information with a personal computer. In another preferred embodiment, communication center **25** is used to flash one or more digital keys or a program onto PAAD **10** using an application that runs on a PC. For example, a user may buy a new door handle compatible with PAAD **10**, and may update the digital key associated with the door handle onto PAAD **10** so that PAAD **10** can work with the new door handle. In this scenario, when the user opens the door handle, the door handle automatically authenticates PAAD **10** and automatically unlocks. When the door handle loses connection with PAAD **10**, the door handle may automatically lock. Flash or flashing is a process for writing data to flash memory. A commonly used process to flash BLUETOOTH devices consists of: using SPI (Serial Programming Interface) protocol and sending/receiving data to BLUETOOTH device through 4 connections: MOSI, MISO, CLK, CSB. The 4 connections (and GND) can be tied directly to ports on the LPT port. Alternatively, the 4 connections are tied to ports onboard a USB to SPI converter, and the USB to SPI converter is connected to USB port onboard the personal computer. A flashing program runs on PED, and sends flashing instructions to either BLUETOOTH chipset directly through SPI protocol, or to USB to SPI converter which in turns sends flashing instructions to BLUETOOTH chipset through SPI protocol. SPI flashing allows to load a new program or to change parameters.

In another preferred embodiment, communication center **25** is used to flash private information such as passwords for different web sites, data bases, computers, etc and associated information onto PAAD **10**. Audio means can be any audio device such as a speaker, a buzzer, a Piezo buzzer, omnidirectional speaker, directional speaker, an ultrasound or any other audio device. Visual means can be an LED, or any visual information display device. Tactile means can be any tactile sensor such as a vibrator, or a heat-generating device.

Antenna **14** can be any type of antenna including chip antenna, patch antenna, PCB antenna and dipole antennas. In another embodiment, antenna **14** is not installed.

In an embodiment, PAAD **10** can be inserted beneath the skin or included inside the housing of objects such as portable computers or RFID badges. It can also be carried as a key-chain or attached to people or objects through a hook, harness, notebook security lock, insert, pin, clip, badge, access card, clip, key chain, car key, firearm activation key, ring, tee, dog collar, Velcro fastener, ring, fastening mechanism, sticky or adhesive surface or any other attachment mechanism. Many notebook computers have a security slot on the side, which can be utilized by inserting a notebook security lock; the lock can be attached to an external device, such as a cable or desktop securing mechanism.

PAAD **10** can also be encased in waterproof packaging and attached to clothes. The packaging can also be shock or impact resistant. System **10** can be incorporated in any other plastic or portable electronic device or object, including for example a cell phone, PDA, a wireless email device, an instant messaging device or pager, a portable computer, an MP3 player, a portable music player, a portable radio device, or any portable electronic device. Preferably, PAAD **10** has dimensions of less than 10 cm×10 cm×5 cm (otherwise stated as "10×10×10 cm") and is less than 200 g in weight. In an embodiment, there are no manually operated controls (e.g., off-on or activation button is magnetically operated, so the housing is not provided with button or switch access), and the device may not have a display. In an embodiment, the housing of the device includes at least one seal and/or is waterproof so that immersion in water, or preferably even running the device through laundering machines, does not damage the electronic components. In a preferred embodiment, system **10** has a size equal to or smaller than 5 cm×3 cm×1.5 cm or 22.5 cubic centimeters ("cc"). A device having the desired functions of the present inventions can fit all of its components into a volume less than 1000 cc, preferably less than about 56 cc, 22.5 cc, and even 10 cc. Each mobile proximity sensor or remote sensor weighs less than 200 grams, preferably less than 50 g, and even less than 10 g. A preferred device has no than four manually operated buttons or switches, and preferably has only one manually operated button or activation switch and no more than one display. Each mobile proximity sensor consumes less than 50 mA.

An embodiment of a remote sensor for attachment to or carrying by a person has no manually operated controls and no display; such an embodiment would be difficult to disable

and particularly durable to operate under robust physical and environmental challenges. Such a device might be carried by soldiers and law enforcement personnel and have a beacon or alarm that is activated should the housing be broken.

FIG. 1B is a schematic of an alternative proximity access and/or alarm device (PAAD) 11 comprising a transceiver system 20 connected with activation switches 13, visual indication center (or display) 16, power store 24, communication center 25, antenna 14, Audio center 18, bearing 23, speaker 27 and capsule 28.

Audio center 18 can be any type of microphone, speaker, earphone wire, etc. In a preferred embodiment, the electronic components of PAAD 11 can be fit into a volume of about 60×30×10 mm or 18 cc or less. For example, PAAD 11 may be fit into a volume less than about 56 cc, 22.5 cc, 18 cc or 10 cc.

Speaker 27 is an earphone, a speaker that fits in the ear or a loud speaker.

Bearing 23 can be a pivot, articulation, U joint, a ball joint, pop-up coil, slide rail, a telescoping tube, or any attachment mechanism for a detachable or movable earpiece. Bearing 23 may be mounted to speaker 27 and may allow adjusting the angle and distance of speaker 27 relative to the main body of PAAD 10 across one or more planes.

Capsule 28 can easily attach and detach to PAAD 11. Capsule 28 allows to protect speaker 27 while not in use. Capsule 28 can attach to a key chain and allows to easily carry PAAD 11 as a key chain when not in use as a headset, and to easily detach it and use it as a headset when needed.

In another embodiment, transceiver system 20 comprises a second BLUETOOTH system that runs AGHFP profile, and that allows transceiver system 20 to function as a relay between a personal electronic device and a headset, thus the user can connection transceiver system 20 to a mobile phone and use all the functions of transceiver system 20, while at the same time use a headset.

Referring to FIG. 2A, in an embodiment, PAAD 10 comprises a transceiver system 20 connected with activation switches 13, visual indication center 16, power store 24, and communication center 25.

Referring to FIG. 2B, in an embodiment, PAAD 11 comprises a transceiver system 20 connected with activation switches 13, visual indication center 16, power store 24, communication center 25, audio center 18, bearing 23, speaker 27 and microphone 29. Microphone 29 is any device capable of capturing voice.

Turning now to FIG. 3A, the flowchart illustrates the steps involved in detecting that a portable electronic device (PED) is outside a desired range of a base device (a base device may be referred to as a master and the monitored remote devices referred to as slaves). The PED can be for example a mobile phone, a PDA, a wireless email device, an instant messaging device, a pager, a portable computer, an MP3 player, a portable music player, a portable radio, or any PED. In step 30, the user activates proximity access and/or alarm device 10/11 by pressing activation switch or button 13.

Activation switch 13 has several modes. In a preferred mode, a long press of activation button 13 on the base unit 10 indicates ON/OFF event. A long press may be defined by either the length of time that switch 13 is manually held in a second position against a bias that holds the switch in a first position when at rest, or a signal may be given to indicate that a desired mode of operation or desired action has been initiated. For example, a very long press can cause a switch to pairing mode. In a preferred embodiment, a double click refers to a long pause.

In another embodiment, activation switch 13 button press can cause one or more messages to be automatically sent to a paired personal electronic device. An application/program running on said paired personal electronic device (PED) perform one or more actions in response to said messages. For example, on a button press, a password and an address (address can be a URL, a link, a phone number, a WAP address, an IP address, a file name . . .) are automatically sent to PED, and a connection to the address is automatically established.

In another embodiment, when PED needs to authenticate the user, PED verifies that paired PAAD 10 is within proximity. PED can either try to establish a Bluetooth connection (HFP/SPP/HID . . .), can page PAAD 10 and wait for a response, or can do an inquiry and verify that a response is received from paired PAAD 10. In a preferred embodiment, PAAD 10 runs as SPP or HFP service. If PAAD 10 does not have voice functionality, then PAAD 10 will first check if paired device supports SPP and if so, PAAD 10 will use SPP. If not, PAAD 10 will connect as HFP. PAAD 10 does not have to implement the full functions of HFP. For example, audio connect, disconnect, forward, etc. do not have to be implemented. If PAAD 11 comprises a microphone and a speaker, then HFP is used.

In step 32, unitary transceiver system 20 in a unitary base unit establishes a BLUETOOTH connection with a monitored remote device. The wireless connection can be a SPP (serial port profile) connection, HSP (headset profile) connection or a HFP (Hands-Free profile) connection. Other connection profiles that can be used include AGHFP (audio gateway HFP), RFCOMM, A2DP (advanced audio distribution profile), AVRCP (audio video remote control profile), AVCTP (audio video control transport protocol), AVDTP (audio video distribution transport protocol), DUN (dial up networking), and GAVDP (general audio video distribution profile).

In one embodiment, messages between said PAAD 10 and said PED may be encrypted using regular encryption algorithms or using digital tones or any other encoding decoding method.

In one embodiment, transceiver system 20 does not redirect voice calls, thus the mobile phone operations remain intact. Transceiver system 20 uses a BLUETOOTH operational mode that uses minimal power, e.g., one of sniff, hold, or park modes. In a preferred embodiment, only BLUETOOTH sniff mode is used after pairing to assure low power usage and optimize convenience to the user by reducing the frequency of battery recharging or replacement.

In sniff mode, a device listens only periodically during specific sniff slots, but retains synchronization with the paired BLUETOOTH device onboard the monitored device. In other embodiments, transceiver system 20 can use hold mode wherein a device listens only to determine if it should become active, or park mode wherein a device transmits its address. Sniff mode assures very low power consumption and thus extends battery life. In sniff mode, a BLUETOOTH master radio frequency unit (e.g., base) addresses a slave radio frequency unit (e.g., remote), which enables the slave to synchronize to the master by sending poll packets and optionally null packets over an active link, the master being arranged so that receipt of a response from the slave unit to a poll packet is sufficient to maintain the active link. The slave unit does not have to respond to all poll packets. This approach can allow the slave to preserve more (transmit) power by going into a deep sleep mode in which a low power oscillator may be used while still allowing the master unit to detect whether the slave has resynchronized or not (and thus to update a Link Supervision Timer, for example).

11

BLUETOOTH Wireless Technology Profiles: In order to use BLUETOOTH wireless technology, a device must be able to interpret certain BLUETOOTH profiles. The profiles define the possible applications. BLUETOOTH profiles are general behaviors through which BLUETOOTH enabled devices communicate with other devices. BLUETOOTH technology defines a wide range of profiles that describe many different types of uses.

At a minimum, each profile specification contains information on (1) dependency on other profiles, (2) suggested user interface formats, and (3) specific parts of the BLUETOOTH protocol stack used by the profile. To perform its task, each profile uses particular options and parameters at each layer of the stack. This may include an outline of the required service record, if appropriate.

Serial Port Profile (SPP). SPP defines how to set-up virtual serial ports and connect two BLUETOOTH enabled devices. SPP is based on the ETSI TS07.10 specification and uses the RFCOMM protocol to provide serial-port emulation. SPP provides a wireless replacement for existing RS-232 based serial communications applications and control signals. SPP provides the basis for the DUN, FAX, HSP and LAN profiles. This profile supports a data rate up to 128 kbit/sec. SPP is dependent on GAP.

Object Push Profile (OPP). OPP defines how to push a file to a BLUETOOTH device. When PAAD 10 is first paired with PED, PAAD 10 can automatically send a file to PED to install drivers and application program necessary for transferring messages and data between PDAP 10 and PED.

RFCOMM. The RFCOMM protocol emulates the serial cable line settings and status of an RS-232 serial port and is used for providing serial data transfer. RFCOMM connects to the lower layers of the BLUETOOTH protocol stack through the L2CAP layer. By providing serial-port emulation, RFCOMM supports legacy serial-port applications while also supporting the OBEX protocol among others. RFCOMM is a subset of the ETSI TS 07.10 standard, along with some BLUETOOTH-specific adaptations.

Hands-Free Profile (HFP). HFP describes how a device can be used to pair, to connect to an audio gateway such as a mobile phone, and to place and receive calls. A typical application is a BLUETOOTH headset device or a BLUETOOTH car kit. Hands-Free Audio Gateway Profile (AGHFP) describes how a gateway device such as a mobile phone can be used to pair, to connect and to send and receive calls to/from a hands-free device. A typical configuration is a mobile phone.

Headset Profile (HSP). The HSP describes how a BLUETOOTH enabled headset should communicate with a computer or other BLUETOOTH enabled device such as a mobile phone. When connected and configured, the headset can act as the remote device's audio input and output interface. The HSP relies on SCO for audio and a subset of AT commands from GSM 07.07 for minimal controls including the ability to ring, answer a call, hang up and adjust the volume.

Advanced Audio Distribution Profile (A2DP). A2DP describes how stereo quality audio can be streamed from a media source to a sink. The profile defines two roles of an audio source and sink. A typical usage scenario can be considered as the "walkman" class of media player. The audio source would be the music player and the audio sink is the wireless headset. A2DP defines the protocols and procedures that realize distribution of audio content of high-quality in mono or stereo on ACL channels. The term "advanced audio", therefore, should be distinguished from "BLUETOOTH audio", which indicates distribution of narrow band voice on SCO channels as defined in the baseband specification.

12

Audio/Video Control Transport Protocol (AVCTP). AVCTP describes the transport mechanisms to exchange messages for controlling A/V devices.

Audio/Video Distribution Transport Protocol (AVDTP). AVDTP defines A/V stream negotiation, establishment and transmission procedures.

Audio/Video Remote Control Profile (AVRCP). AVRCP is designed to provide a standard interface to control TVs, hi-fi equipment, or other A/C equipment to allow a single remote control (or other device) to control all the A/V equipment that a user has access to. It may be used in concert with A2DP or VDP. AVRCP defines how to control characteristics of streaming media. This includes pausing, stopping and starting playback and volume control as well as other types of remote control operations. The AVRCP defines two roles, that of a controller and a target device. The controller is typically considered the remote control device while the target device is the one whose characteristics are being altered. In a "walkman" type media player scenario, the control device may be a headset that allows tracks to be skipped and the target device would be the actual medial player.

This protocol specifies the scope of the AV/C Digital Interface Command Set (AV/C command set, defined by the 1394 trade association) to be applied, realizing simple implementation and easy operability. This protocol adopts the AV/C device model and command format for control messages and those messages are transported by the Audio/Video Control Transport Protocol (AVCTP).

In AVRCP, the controller translates the detected user action to the A/V control signal, and then transmits it to a remote BLUETOOTH enabled device. The functions available for a conventional infrared remote controller can be realized in this protocol. The remote control described in this protocol is designed specifically for A/V control only.

Dial-up Networking Profile (DUN). DUN provides a standard to access the Internet and other dial-up services over BLUETOOTH technology. The most common scenario is accessing the Internet from a laptop by dialing up on a mobile phone wirelessly. It is based on SPP and provides for relatively easy conversion of existing products through the many features that it has in common with the existing wired serial protocols for the same task. These include the AT command set specified in ETSI 07.07 and PPP.

Like other profiles built on top of SPP, the virtual serial link created by the lower layers of the BLUETOOTH protocol stack is transparent to applications using the DUN profile. Thus, the modem driver on the data-terminal device is unaware that it is communicating over BLUETOOTH technology. The application on the data-terminal device is similarly unaware that it is not connected to the gateway device by a cable. DUN describes two roles, the gateway and terminal devices. The gateway device provides network access for the terminal device. A typical configuration consists of a mobile phone acting as the gateway device for a personal computer acting as the terminal role.

General Audio/Video Distribution Profile (GAVDP). GAVDP provides the basis for A2DP and VDP, the basis of the systems designed for distributing video and audio streams using BLUETOOTH technology. GAVDP defines two roles, an initiator and an acceptor. In a typical usage scenario, a device such as a "walkman" is used as the initiator and a headset is used as the acceptor. GAVDP specifies signaling transaction procedures between two devices to set up, terminate and reconfigure streaming channels. The streaming parameters and encode/decode features are included in A2DP and VDP which depend on this profile.

13

In step 33, transceiver system 20 monitors the BLUETOOTH connection automatically. In this step, transceiver system 20 is in sniff mode, and power consumption is below 1 mA. A significant benefit of this system is the ability to monitor a connection while keeping power consumption to a very low level. This enables one of ordinary skill in the art to build portable devices in accordance with the present inventions that use small batteries (100-200 mAh), which can last for at least 2 or 3 weeks before being recharged or swapped. In step 34, on detection of connection drop, i.e., disconnection, transceiver system 20 attempts to reconnect in step 36. For example, when a connection is dropped while the system is in sleep mode or sniff mode, a BLUETOOTH system can automatically generate an event indicating connection drop. In the base and/or remote devices of the present invention, upon the BLUETOOTH system indicating a connection drop either the base and/or the remote will attempt to reconnect to one another or an alarm will be triggered in the base and/or the remote, as illustrated by issuance of an alarm in step 40. For a mobile phone, a connection drop is generally due to one of the followings:

- The distance between transceiver system 20 and the mobile phone is too large,
- There is an obstacle between the two devices. The obstacle prevents communication,
- The mobile phone is powered down,
- Several mobile phones are not able to support more than one active BLUETOOTH connection and drop existing BLUETOOTH connections when a user activates a new BLUETOOTH device such as a headset.

To avoid problem with headsets, PAAD 10 has the following methods have been tried:

- In a less preferred embodiment, when a connection drop is detected, PAAD 10 pages the user headset to see if the headset is active, and if so, the alarm will not go ON. This method is not compatible across different headsets as many headsets do not respond to paging when a call is active.
- In another less preferred embodiment, when a connection drop is detected, PAAD 10 pages the mobile phone to see if the mobile phone is in the vicinity, and if so, the alarm will not go ON. This method is not compatible across different mobile phones as many mobile phones do not response to paging when a headset is active.
- In another preferred embodiment, PAAD 10 runs 2 BLUETOOTH profiles simultaneously: HFP and AGHFP, and connects to PED and to headset when headset is active. This method works, voice may experience some cracking as the processor power is split over two devices.
- In another preferred embodiment, PAAD 10 comprises 2 Bluetooth transceivers. One connects to PED and the other connects to headset when headset is active. This solution works well but requires a higher cost and battery consumption.
- In another preferred embodiment, PAAD 10 has a sleep mode that the user can initiate by pressing activation switch 13. This mode allows PAAD 10 to sleep for a predetermined duration, without alarm or reconnection to PED, and to resume monitoring PED after the duration is expired. This solution, although not very elegant, solves the problem with headsets in a cost effective manner.

One of ordinary skill in the art will understand from the foregoing that the firmware of the BLUETOOTH system can be programmed to include instructions to reconnect and/or to trigger an alarm in accordance with the present invention. Automatic reconnection minimizes false alarms and makes the systems of the present invention more reliable and easy to use. An exemplary benefit of the automatic reconnect feature

14

is that when a user comes within proximity of the mobile phone from out of range, the alarm automatically shuts off without requiring any additional input from the user.

Furthermore, the alarm when activated, may go on and off periodically following a first short period, however, after a predetermined period of alarming, the periodic short period may be changed to a periodic long period so that the system battery is not drained quickly.

In another embodiment, automatic reconnect can be used to trigger an audible alarm for indicating a paired device has come into proximity.

In an embodiment of the present inventions, the BLUETOOTH system will generate an indication or message on detection of a connection drop. For example, firmware running on a BLUETOOTH chipset, or on a virtual machine which in turn runs on a BLUETOOTH chipset, can receive or capture that disconnect indication or message. The present invention includes programming that instructs one or more responses to a disconnect indication. For example, the program will instruct a reconnection attempt and/or instruct issuance of an alarm. One of ordinary skill in the art can use market available development tools to write programming to perform the desired functions. It has been discovered by the present inventor that the disconnect event indicator is reliable for detecting that a monitored device is outside a desired range. The claimed invention has an automatic reconnect attempt feature, so that upon detection of a disconnect event, reconnection is attempted; this can avoid many false alarms. Preferably, in an embodiment, an alarm instruction is not given until at least one active reconnect attempt is made and fails. Upon the alarm issuing, periodic reconnect efforts are made, and upon reconnection the alarm will not continue. Furthermore, the claimed invention has a sleep mode that the user can initiate to prevent the alarm mode. Many PED devices on the market only allow one BLUETOOTH device to be connected at any time, and this creates conflict with PAAD 10. The sleep mode allows the user to put PAAD 10 in sleep mode in order to connect other BLUETOOTH devices to PED for a duration of time. For example, if the user wishes to use a headset, the user can put PAAD 10 in sleep mode before using the headset. After the duration of time elapses, PAAD 10 automatically resumes operation. If the sleep mode is not ON and the user activates a Bluetooth headset, with some mobile phones, PAAD 10 may start alarm when the headset is ON and the headset operation may be interrupted due to PAAD 10 trying to reconnect. Avoidance of false alarms makes the invention more convenient for the user.

In an embodiment, the automatic reconnection feature enables the user to locate lost keys that are connected to PAAD 10 of the present inventions. Turning the mobile phone off automatically triggers an alarm on the key chain device and helps one to locate the keys.

Referring again to the Figures, upon a monitored PED leaving a desired proximity, processor of transceiver system 20 can start a buzzer, a vibrator, or a sound system. Processor of transceiver system 20 can also activate LEDs. An example of an audible warning message could loudly state "Your phone is no longer in authorized area". In a preferred embodiment, after an alarm is issued in step 40, system 20 regularly attempts to reconnect with the monitored device.

Turning now to FIG. 3B, the flowchart illustrates the steps involved in detecting that a portable electronic device is outside a desired range and for transmitting or receiving voice.

Since most people prefer to limit the number of devices they carry on them, this preferred embodiment allows adding BLUETOOTH headset functionality to PAAD 11. When speaker 27 is folded/pulled/pushed/twisted/rolled/slid

15

around bearing 23, the system automatically functions as a BLUETOOTH headset. Speaker 27 can also pivot, roll or slide around bearing 23 in order to provide better fit and comfort.

When speaker 27 is unfolded, pulled, slid . . . , the system is a flat device that can be carried as a key chain. The system automatically functions as a PAAD 10 key chain that monitors proximity to a PED and issues alarm in case PED is not within proximity. PAAD 10 can either use SPP or HFP when in alarm mode. PAAD 10 connects with capsule 28 for easy carrying as a key chain. This design allows the user:

- To have a quick access to a BLUETOOTH headset,
- To carry the BLUETOOTH headset as a keychain,
- Alarm when phone is not in proximity,
- System automatically reconnects when phone is in proximity, and alarm automatically shuts off,
- To adjust the ear piece for better comfort,
- The ear piece is shielded when not in use by inserting it in a key chain part,
- The keychain can secure access to the mobile phone, and if keychain is not within proximity, the mobile phone cannot be unlocked,
- The keychain can secure access to applications onboard the mobile phone, and if keychain is not within proximity, the access to the application cannot be granted.
- The keychain can hold decryption keys for decrypting sensitive data onboard the mobile phone,
- The keychain can hold several functions such as a Bluetooth memory, flash memory, USB Flash drive, MP3/MP4 player, recording device, bio sensor, comb, flash light, lighter, home key, car key, firearm activation, key, Swiss knife, inter alia

Most BLUETOOTH headsets on the market:

- Do not have a convenient way to carry them, except by attaching them to the ear,
- Have a fixed angle between the ear piece and the main body of the device,
- Have a cover for the ear piece that is small and not practical. It also gets lost easily.

In another embodiment, the microphone comprises an extendable arm. The extendable arm can fold, rotate or slide. This allows for a smaller size for the main part, as well as good microphone voice capture capability.

In another embodiment, the battery is removed from the main body of the device and placed in a second part, such as a lid. This makes the BLUETOOTH headset lighter and smaller considering that a battery generally accounts for more than 60% of components volume. When inserted into the lid unit, the capacitor onboard the main body recharges.

In step 321, the system is in voice mode. The user may select voice mode by folding, pulling, sliding, twisting speaker 27. In step 323 the system receives voice from PED and sends it to its onboard speaker. In step 324, the system sends voice from an onboard microphone to PED. The system uses HFP protocol to send voice to/from PED.

In step 322, the system is in alarm mode.

In a preferred embodiment, if an event is detected selected from:

- single button press, double button press, multiple button press,
- switch activation,
- voice command, sound command,
- shaking device,
- removing device cover,
- folding device;

The system goes to sleep for a period of time selected from 30 minutes, 60 minutes, or any number of minutes.

16

Turning now to FIG. 4, the flowchart illustrates initiating the proximity access and/or alarm device. In step 42, PAAD 10 enters pairing mode. In step 44, visual indication center 16 can indicate pairing mode using a combination of LED effects, for example, alternating colored LEDs. When transceiver system 20 is set to discoverable mode, in accordance with step 46 the user uses a second BLUETOOTH PED to be monitored to search for BLUETOOTH devices in range and to select the PAAD 10 from the search list.

When the user initiates a pairing request, as shown in step 48, PAAD 10/11 receives a pairing request from a second device, and requests a PIN code. On successful pairing in step 50, PAAD 10 obtains the BLUETOOTH address of second device and stores it in memory as shown by step 52. Transceiver system 20 changes to non-discoverable mode and visual information center 16 changes to normal mode.

In another embodiment, after pairing, transceiver system 20 may send a file to second BLUETOOTH device using OPP profile. This file can be one or more promotional files such as a brochures, music, video, or application software such as a driver, a game, a client application, etc.

Turning now to FIG. 5, the flowchart illustrates an alternative embodiment using an application onboard the monitored device. The client application is used to configure PAAD 10/11. In step 54, an application running on PED obtains configuration parameters. Configuration parameters include digital keys, passwords, as well as operation hours, operation days, buzzer type, buzzer volume, buzzer duration, range and alarm type. PAAD 10/11 is connected to PED through an interface cable that connects USB or LPT port on the PED to communication center 25 on PAAD 10/11.

The configuration parameters can be supplied through an application or through a remote administration console and are stored or flashed onboard PAAD 10/11 in step 56 and can be used to change the properties or the program of PAAD 10.

On detection of a connection drop, PAAD 10 periodically attempts to reconnect, and on failure, activates an alarm. In an embodiment, the range of PAAD is less than about 15 meters, less than about 20 meters or less than about 4 meters.

In another embodiment, on detection of a connection drop, PED periodically attempts to reconnect, and on failure, activates an alarm. In an embodiment, the range of the PED is less than about 15 meters, less than about 20 meters or less than about 4 meters.

In another embodiment, PAAD 10 can pair with PED and also with a number of other PAAD 10s. The original PAAD is configured so that it will not alarm if any of PED or the other PAADs are within proximity.

This allows the user to place some of the other PAADs at known locations, such as around the house, or office. This would prevent PAAD from providing a false alarm when the user is around known locations, or to cover some blind spots.

In another embodiment, proximity access and/or alarm device 10/11 has a PC lock insert that is used to lock the system to the side of a computer laptop or attaches to a laptop carry case. The alarm onboard proximity access and/or alarm device 10 is triggered when the laptop is more than a predetermined distanced from a mobile phone that has a paired BLUETOOTH system. Therefore, it prevents the laptop from being lost, forgotten or stolen. Preferably the alarm is triggered when the PC and the mobile phone are less than 10 meters apart.

Turning now to FIG. 6, the flowchart illustrates an alternative embodiment for providing secure access to encrypted data.

The user starts an application to access sensitive data in step 80. The user enters a password in step 81 and if validated

17

in step 82, PED establishes a secure Bluetooth 2-way wireless connection with PAAD 10 in step 83.

In step 84, one user requesting data, PED sends a message to paired device in step 85.

In a preferred embodiment, PAAD 10 stores a part of a private key. Also, the message sent by PED may contain an obfuscation formula, for example, a large random number and a code for an obfuscation formula.

pK = private key
 ppK = part of private key
 oppK = obfuscated part of private key stored on mobile device
 r = random number generated by PED
 f = obfuscation function
 cf = code for obfuscation formula generated by PED
 l = data sent from PED to PAAD
 >> l = r, cf

(cf) changes every time or periodically. PAAD 10 knows how to interpret (cf) and convert it to a function.

(r) is a random string or number. For example, a 128 byte string or number. Function (f) may be: ADD, DELETE, MULTIPLY, SHIFT ONE BIT THEN ADD, AND, OR, NAND, NOR, APPEND, REVERSE THEN ADD, COMBINE BIT . . .

Function (f) may be applied to (r) and to (oppK) and the result of the function is sent to PED. PAAD 10 must be programmed with the codes (cf) and associated obfuscation/transformation.

PED awaits receipt of key in step 86 in real-time, i.e. within a predetermined period (such as 0.5 second or less than 1 second).

O = data sent from PAAD to PED
 >> O = f(r, oppK)

In step 87, PED de-obfuscates or decrypts received key.

f* = reverse of obfuscation function
 oppK = f*(O, r)

PED can also de-obfuscate (oppK) to obtain (ppK).

In step 88, PED uses (ppK) as well as information from user password to obtain private key (pK).

The application may extract a second part of private key from pre-known positions of the user password and use the first part and second part to form a private key. (In this case, at initiation of a user password, the user is given some codes that he/she must use as part of a personal password and at specific positions. These codes represent part of the private key. For example, the user is given a choice for the first 5 digits of a password, and is instructed to use 3 specific digits at the end. Another example, is the user must use 4 specific digits at the front, and 4-6 own digits next. Another example is the user is given a specific password, etc. . . .).

In a preferred embodiment, the user is asked for password the first time sensitive data is requested, but after that, authentication is done wirelessly in real-time without requesting information from the user, thus the process is unobtrusive to the user.

In step 89, it uses the private key to decrypt encrypted data and to provide it to the user.

It is important to note that the key is generated in real-time every time encrypted data is requested, and that the key is not

18

stored in memory for a long period (more than the time required to decrypt the data) and is not stored on data storage device.

It is also important to note that decrypted data is not written to data storage device.

If user requests more data, the key is generated again, and more data is decrypted. Furthermore, if the user requests a data volume larger than a predetermined amount, then only predetermined amount is decrypted. Also, if the user requests more data than available RAM memory, then only volume of data that can be kept in available RAM memory is decrypted. This ensures that decrypted data is never stored on data storage device.

PED can also request a digital key from PAAD 10. If a positive response is received, user access to PED is authorized, and if not, user access is denied.

For example, on user activating a mobile phone or a firearm device, the mobile phone will check that PAAD 10 is within proximity. If confirmed, the phone is unlocked and the user does not have to enter a password.

Another example is on user pressing a keyboard key; the computer will check that PAAD 10 is within vicinity. If confirmed, the computer will automatically log the user in and the user does not have to enter a password in the Windows password screen. In this example, the wireless range of PAAD 10 may be reduced to minimum range. A Class 3 Bluetooth transceiver may be used or the antenna may be removed so that PAAD 10 has minimum range. If the computer finds more than one authorized user in its vicinity, the computer may ask the user for further authentication or challenge questions.

In another embodiment, a sensitive information application onboard mobile phone for example, checks that PAAD 10 is within proximity. If confirmed, the user is granted access to the application, or data can be decrypted.

In another embodiment, on user trying to access a protected address such as a URL or link, a protected file, an encrypted file, an encrypted record, or a protected database, an application/program running on said paired PED sends a message to said PAAD 10 requesting a digital key. The message may include an address for which a password is sought. Said PAAD 10 automatically sends said digital key. Said digital key may be input in the appropriate fields for authentication or decryption.

This method has the following advantages:

- 1—Real-time: all the operations can be performed in real-time
- 2—Simple: uses simple processing and does not require any processor with more than 100 MIPS or more. All operations can be performed by a microcontroller or small power processor
- 3—Secure channels: channels used a secure using Bluetooth security and it is difficult for hackers to copy the data transmitted
- 4—Time bound: response to a specific operation must be given within a very short time (less than one second) of sending the operation. It would be impossible for a hacker to interpret the transformation method and send a response in the allocated time period
- 5—The sent message consisting of a very large random number, a very small changing operation code, and a changing transformation method, results in a random result sent from PAAD 10 to PED with no obvious relationship to the sent message. The larger the number of obfuscation/transformation methods, the harder it is to find any relationship between the received message and the generated message

19

6—The key is not stored on the same physical medium as the data

7—A portion of the key is held on a mobile device, and the other portion is extracted from the user, thus even if the mobile device is cloned without the user knowing, the mobile device cannot be used to access the data directly

8—A periodic check with a remote server is performed to ensure that PED and PAAD 11 have not been stolen together. If a thief steals both PED and PAAD 11, the thief has a limited window of time to decode the second part of the private key. One the periodic check with remote server is performed, PED will be instructed to self-destroy. Also, in the absence of successful connection, PED will either destroy sensitive data.

a. In a preferred embodiment, PAAD 10 is used to store a part of a private key in a separate location from sensitive data and to supply it to decryption interface in real time when needed to be used as a decryption key. PAAD 10 provides a secure and safe location to store a private key, a part of a private key, or an obfuscated private key/part of a private key in a way that provides far better security and hacker safe system than any other available method.

b. The private key is made completely hacker proof by partitioning it in multiple parts, obfuscating/encrypting a part of the private key and storing it on a mobile device. Furthermore, communication with mobile device is made safe by ensuring close to random data transmission between PED and the mobile device, and close to random data transmission between the mobile device and PED. The correlation factor between the data sent from the PED to the mobile device and the data sent from the mobile device to PED is kept close to a minimum by using the following formulas:

c. When PAAD 10 is paired with PED, it becomes undiscoverable, and will never be able to pair again unless re-flashed through communication center 25. This ensures that PAAD 10 can only be used with one or more PEDs to which it was originally paired and if lost, it cannot be used to access or decrypt data on any other PED. Also, when PAAD 10 is lost, the user/administrator can un-pair PED from a PED console or from a remote console. The lost PAAD 10 will no longer cause any security threat to PED or to other PEDs. Furthermore, information onboard PAAD 10 is obfuscated or encrypted so that a hacker cannot use it. Information onboard of PAAD 10 is a part of private key which is not useful unless it is de-obfuscated, decrypted, and combined with another part of private key extracted from a user password.

d. These methods provide for a very secure data access method, or a data decryption system and method that cannot be breached even when a PAAD 10 device is lost.

In case of unauthorized access, the data will be encrypted and cannot be opened unless in the absence of PAAD 10 which supplies a part of the private key and of the user who supplies a password containing another part of the private key. Furthermore, viruses, Trojan Horses and spywares are ineffective because the data on the storage device or solid state memory is encrypted.

The present invention also secures content onboard the portable electronic device. It presents a comprehensive solution that ensures that content is protected to a maximum level, and cannot be tampered with. This solution involves minimum effort on the part of the user, and ensures minimum risk

20

of exposure in case of a theft of a personal electronic device or a proximity access and/or alarm device occurs.

Public-key infrastructure (PKI) ensures that people are who they say they are and also proves that documents haven't been tampered with.

PKI uses extremely long prime numbers, called keys. In preferred embodiment, keys are 128 bytes long or longer. Two keys are involved—a Private Key, which the owner of the information has access to, and a Public Key, which can be accessed by anyone. The two keys work together, so a message scrambled with the Private Key can only be unscrambled with the Public Key and vice versa. The more digits in these keys, the more secure the process.

A large piece of data set to be encoded—for instance, a document—is run through a complicated mathematical computation to generate a single large number, called a hash. The original data and the hash are inextricably linked. If either changes, the hash won't match. Any entity can verify the validity of the document by checking a stored hash against a hash computed from the data. If the hashes match, the data was not tampered with.

Since the present invention seeks to protect PED as well as data onboard PED, Public Key infrastructure (PKI) is used to generate a set of Public Key and Private Key unique for each user. A proximity access and/or alarm device (PAAD) 10 is assigned to each user for storing the Public Key (or alternatively the Private Key), and an application/driver/program/chipset/plugin/file manager/data base manager containing the Private Key (or alternatively the Public Key) is installed on the user PED.

Sensitive data on PED storage medium (hard drive, solid state memory, Flash, network drive, CD Rom, Zip drive, Bluetooth drive) is kept encrypted at all time, using Private Key (or alternatively the Public Key). A hash may be generated and stored every time the data is updated.

On user request to read data, a request is made to PAAD 10 to get the Public Key, and the requested data is decrypted using the key. The requested data is presented through an authorized application. The hash may be generated again and compared with the stored hash key to ensure the data has not been tampered with.

When the user request data, the hash key for the data may be validated against the old hash key to ensure the data has not been tampered with.

Turning to FIG. 7, the flowchart illustrates the operation of a Bluetooth key. In step 90, a user activates a button onboard PAAD 10. In step 92, PAAD 10 established a Bluetooth connection with access point. Access point may be any door, lock, vault In step 94, the access point validates the public key. If validated in step 96, access point authorizes access in step 98 and activates lock mechanism in step 99.

Recovery strategy: when the owner of the lost or stolen PAAD 10 reports the lost or stolen device, the administrator (or the user) can:

Pull the old Private Key from a safe place,

Assign a new PAAD 10 (with a new BLUETOOTH ID),

Put the old Private Key on the new PAAD 10 (by flashing it through communication center 25),

Un-pair PED from the old PAAD 10, (this can be done either on the PED, or by remote accessing the PED)

Send the new PAAD 10 to the user,

Pair PED with the new PAAD 10, (this can be done by activating PAAD 10, and entering PIN code on PED)

Since the old PAAD 10 is unpaired from PED, the user of the old PAAD 10 will not be able to use it with associated PED.

21

However, since the user Private Key is stored on the lost/stolen PAAD 10, it is a better procedure to also:

Assign a new Public Key and Private Key to the user,
Store the new Private Key on the new PAAD 10, (by flashing it through communication center 25)

Decrypt all previously encrypted data using old Private Key, and encrypt it again using the new Public Key before storing it onboard PED.

In case the PED and PAAD 10 are stolen together, the sensitive data may be compromised unless further security is built such as the followings:

For added security, PED connects automatically to a remote server (periodically or at random intervals) and collects messages. If remote server indicates breach of security, said PED deletes the private keys or destroys/deletes date. Also, if connection to remote server is not possible, the user is given a deadline to enable connection. If the deadline is passed and the connection is not provided, PED deletes the private key.

In another preferred embodiment, 2 PAAD 10 devices are used to secure a PED and data onboard. A first PAAD 10 is carried by the user as a keychain or badge, and is used to authenticate access to data (and decrypt data) onboard PED based on user proximity to PED. A second PAAD 10 is attached to PED carry case, and is used to monitor proximity to first PAAD 10, and alarm when said proximity is breached.

In another embodiment, PAAD 10 includes an encryption/decryption chipset for running public/private encryption to secure communication between PED and PAAD 10.

Turning now to FIG. 8, the flowchart illustrates an embodiment for setting up PAAD 10 and associated PEDs.

The administrator generates a set of unique private key and public key for a user in step 100. The administrator can be a person or an automatic program. The private key is flashed on PAAD 10 in step 101, and then stored in a safe place in step 102. The public key is used to encrypt data that is stored on a data storage device and accessed using PED in step 103. The public key is also used to encrypt information that is sent to PED, either through network download, email, flash drive, CD, DVD, or any other means. The administrator may install an application on PED to view the sensitive data in step 104. The PED and PAAD 10 are paired in step 106. The PED and associated PAAD 10 are transferred to the final user in step 108. Traditionally, The PED and PAAD are sent separately.

Several keys may be stored on PAAD 10. These keys can be used to access multiple secured applications or multiple data within an application. Different keys can also govern different access privileges such as read, write, delete, modify for different pieces of data.

If the user requires access to more than one PED, the public keys for all those computers can be flashed on PAAD 10 and PAAD 10 is paired to those PEDs.

The private key is stored on a device that is on the user most of the time, such as a badge or a key chain, thus reducing the risk of theft of the key if the PED is stolen. This is in contrast to a USB key which must be kept with the PED when it is used, and can be stolen with it.

On user request to update/save/write sensitive data on storage medium, if the user is granted write privilege, data is automatically encrypted using the Public Key and written to storage medium. The hash key is regenerated and stored. The write privileges may be obtained from PAAD 10. In case the PED is stolen, PED is lost, a Trojan Horse is installed onboard PED, a virus/impostor/unauthorized user tries to access the data onboard PED, the sensitive data will be encrypted and will be very difficult to decrypt.

22

This invention consists of event-based Real-time decryption on the fly, of a fixed-size set of data, with no storing of decrypted data on disk, using a FOB that comprises only a single Bluetooth transceiver IC, module or chip. The FOB contains no other transceiver, no transmitter/receiver not other processor than the arm processor of the BLUETOOTH IC, no RFID, no GPS receiver, no GSP modem, no pager modem, no LCD, no other memory besides the memory of the transceiver module. BLUETOOTH ICs are generally available from CSR, Broadcom or other manufacturers and comprise a small RISC processor, limited RAM, ROM or Flash memory.

The decryption can be driven by events such as a user scrolling down on a page, the user opening a file, the user searching a record, the user clicking on a record, or any user event. In a preferred embodiment, the functionality is built into Application Programming Interfaces (APIs) and supplied to programmers. The programmers will choose where the validation points take place, either on initiation, on a record by record basis, on a size basis, on a time basis, or a button click basis, on a user basis, time of day, type of data, or any logical point.

User program can be loaded on the Flash memory or engraved in ROM.

In another preferred embodiment, we combine a physical key with public key/private key security with headset functionality to provide the next generation key that not only opens doors (car door, home door, garage door, vault door), but also provides headset voice capability. The motivation behind this is:

- 1—Users do not want to carry any extra devices besides car key and mobile phone.
- 2—Cars nowadays offer voice solutions when the user is inside the car, and it would be more interesting for them to provide a total solution, regardless of where the user is.
- 3—Cars keys are becoming a small electronic device with the event of RFID.
- 4—Most drivers use mobile phones.
- 5—Most drivers need or will need to comply with hands free legislation.
- 6—Users should have their keys and their mobile phone in proximity most of the time.
- 7—More importantly, most people that use a remote control for unlocking a car, have to first press a button onboard the remote control, then pull the door handle. These 2 steps can be merged by just doing one step, that of pulling the door handle. The handle should be able to automatically authenticate the key, and allow access. In other terms, access is only granted if PAAD 10 is in proximity.

In a preferred embodiment, the key chain with PAAD 10 functionality is integrated with a headset piece. The headset piece is rotating so that the key can be flat when it is not inserted in the ear, and can have the shape of a headset when folded. PAAD 10 can include a metal key to be used in case onboard battery is out of charge.

In another embodiment, PAAD 10 can charge its battery from a vehicle's ignition system, whereby when PAAD 10 is placed in the ignition system, it recharges.

Further, for more security, the user may provide biographic authentication such as be not limited to voice recognition, password entry, retinal scan, finger print, or other information.

Since most people carry a wallet, a mobile phone and keys, PAAD 11 provides a user with valuable all in one features and

23

at the same time does not require the user to carry and extra device, all this thanks to Bluetooth. The features include:

- Proximity alarm for mobile phone
- Headset for mobile phone
- Locator for parked vehicle
- Vehicle keys
- Door keys

The details of certain embodiments of the present inventions have been described, which are provided as illustrative examples so as to enable those of ordinary skill in the art to practice the inventions. The summary, figures, abstract and further details provided are not meant to limit the scope of the present inventions, but to be exemplary. Where certain elements of the present inventions can be partially or fully implemented using known components, only those portions of such known components that are necessary for an understanding of the present invention are described, and detailed descriptions of other portions of such known components are omitted so as to avoid obscuring the invention. Further, the present invention encompasses present and future known equivalents to the components referred to herein.

The inventions are capable of other embodiments and of being practiced and carried out in various ways, and as such, those skilled in the art will appreciate that the conception upon which this disclosure is based may readily be utilized as a basis for the designing of other methods and systems for carrying out the several purposes of the present inventions. Therefore, the claims should be regarded as including all equivalent constructions insofar as they do not depart from the spirit and scope of the present invention. The following claims are a part of the detailed description of the invention and should be treated as being included in this specification.

The invention claimed is:

1. A unitary mobile apparatus, comprising:

a short wireless transceiver,

a port means selected from the group consisting of:

- a USB connector, a mini USB connector and a data port;
- wherein said port means can operatively connect to a remote computer,

- wherein a flashing program running on said remote computer can write at least one code corresponding to a user account to a flash memory onboard said unitary mobile apparatus when the remote computer is operatively connected to said unitary mobile apparatus;

whereby after said unitary mobile apparatus receives at least one transformation directive wirelessly from a paired second apparatus, at least one obfuscation function is applied to at least one first message resulting in at least one encoded message,

- wherein the at least one transformation directive is different from a previously received second transformation directive,

- wherein said unitary mobile apparatus automatically transmits the at least one encoded message wirelessly to the paired apparatus.

2. The apparatus of claim 1, wherein:

- upon detection of a connection drop from a paired second apparatus, said unitary mobile apparatus periodically attempts to reconnect to the paired second apparatus.

3. The apparatus of claim 2, further comprising:

- an alarm audible from at least 0.5 meter distance from the unitary mobile apparatus;

- wherein said alarm is activated after a connection between said unitary mobile apparatus and the apparatus drops.

24

4. The apparatus of claim 1, wherein:

- the unitary mobile apparatus fits into a space having a volume less than 18 cubic centimeters.

5. The apparatus of claim 1, further comprising an earpiece selected from the group consisting of:

- a foldable earpiece for voice communication,
- a pull-up earpiece for voice communication,
- a telescopic earpiece for voice communication,
- a rotating telescopic earpiece for voice communication,
- and a slide earpiece for voice communication.

6. The apparatus of claim 1, wherein said apparatus does not comprise a cellular transceiver.

7. A method for accessing data from a first device using digital keys stored on a unitary mobile apparatus, comprising the steps of:

- connecting an external port means onboard the unitary mobile apparatus to a remote computer;

- using a flashing program on the remote computer to write at least one pass code corresponding to a user account to a flash memory onboard the unitary mobile apparatus;
- whereby after receiving a request to decrypt encrypted data on the first device,

- sending a transformation directive to the unitary mobile apparatus using short range wireless communication, wherein the transformation directive identifies a first obfuscation code for a first obfuscation function stored onboard the unitary mobile apparatus,

- wherein the transformation directive is different from a previously sent second transformation directive;

- whereby after receiving a wireless reply from the unitary mobile apparatus and wherein said wireless reply comprises at least one encoded digital key,

- applying a first reverse function corresponding to said first obfuscation function,

- wherein said first reverse function reverses the obfuscation of the first obfuscation function to obtain at least one decoded digital key corresponding to the at least one encoded digital key,

- and using the at least one decoded digital key to decrypt the encrypted data.

8. The method of claim 7, wherein every time a transformation directive is sent, a different obfuscation code is used.

9. The method of claim 7, whereby:

- upon receipt of a transformation directive from a paired apparatus, said transformation directive comprises a first obfuscation code for a first obfuscation function, automatically applying said first obfuscation function to at least one digital key, and automatically transmitting the transformed at least one digital key to the paired apparatus wirelessly.

10. The method of claim 7, whereby:

- if said encrypted data exceeds a predetermined size, decrypting a first part of said encrypted data and displaying the first part of the decrypted data,
- after obtaining a user request for a next set of data, decrypting the next part of said encrypted data and displaying the next part of the decrypted data.

11. The method of claim 10, wherein said first part of the decrypted data part is not written to a data storage device.

12. The method of claim 7, further comprising:

- the personal electronic device periodically connecting to a remote server, requesting a validation code, and, if a validation code is not received within a predetermined time,

- the personal electronic device deletes said decrypted data.

25

13. The method of claim 7, further comprising:
connecting the unitary mobile apparatus to a personal com-
puter using a data cable, and flashing one or more digital
codes on the unitary mobile apparatus.
14. The method of claim 7, further comprising: 5
encrypting data using a key, and
storing the encrypted data onboard a storage device.
15. The method of claim 7, comprising:
obtaining an old private key and an old public key,
generating a new private key and a new associated public 10
key,
decrypting said data using said old private key or said old
public key, and
encrypting said data using said new private key or said new
public key. 15
16. A method for access using digital keys stored on a
unitary mobile apparatus, comprising:
connecting an external port means onboard the unitary
mobile apparatus to a remote computer;
using a flashing program to write digital keys correspond- 20
ing to a user account to a flash memory onboard the
unitary mobile apparatus;
whereby, after receiving a request to decrypt encrypted
data on onboard an electronic device

26

- establishing a secure two-way short wireless connection
between the electronic device and the unitary mobile
apparatus,
transmitting at least one transformation directive wire-
lessly from the electronic device to the unitary mobile
apparatus,
wherein the at least one transformation directive is dif-
ferent from a previously received second transforma-
tion directive,
whereby, after receiving a valid response from the unitary
mobile apparatus, the electronic device automatically
activates a lock.
17. The method of claim 16, whereby:
upon detection of a connection drop,
the electronic device automatically activates the lock.
18. The method of claim 17, further comprising:
connecting the unitary mobile apparatus to a personal com-
puter using a data cable, and flashing one or more digital
codes on the unitary mobile apparatus.
19. The method of claim 16, whereby:
upon connecting the unitary mobile apparatus to an igni-
tion system, a battery onboard the unitary mobile appa-
ratus charges.

* * * * *